A Framework for Data Sharing between Healthcare Providers using Blockchain

Ahmed G. Alzahrani[1,2], Ahmed Alenezi[1,3], Hany F. Atlam[1] and Gary Wills[1]
[1]Electronic and Computer Science Dept., University of Southampton, University Road, SO17 1BJ, Southampton, U.K.
[2]Department of Computer Science, Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah 21589, Saudi Arabia
[3]Computer Science Dept., Faculty of Computing and Information Technology, Northern Border University, Arar, K.S.A.

Keywords: Blockchain, Healthcare Systems, Sharing Data, Privacy, Security, Kingdom of Saudi Arabia.

Abstract: The healthcare data are considered as a highly valuable source of information that can improve healthcare systems to be more intelligent and improve the quality of the provided services. However, due to security and privacy issues, sharing data between healthcare organisations is challenging. This has led to data shortage in the healthcare sector which is considered as a significant issue not only in the Kingdom of Saudi Arabia (KSA) but also worldwide. The primary objective of conducting this paper is to investigate the various factors that enable secure sharing and exchange of healthcare information between different healthcare providers in the KSA. It starts by discussing the current literature and frameworks for managing healthcare data information and the challenges that health providers encounter, particularly when it comes to issues such as data security, patient privacy, and healthcare information exchange. These challenges in managing healthcare data have necessitated the need for implementing a solution that can allow medical providers to have access to updated healthcare information. Attention in the healthcare sector has been drawn to blockchain technology as a part of the solution, especially after the technology was successfully applied in the financial sector to improve the security of financial transactions, particularly involving digital currencies such as Bitcoin. Therefore, a framework based on the blockchain technology has been proposed to achieve the goals of the present research.

1 INTRODUCTION

Advancements in Health Information Technology (HIT) have resulted in improved delivery of healthcare services to consumers as well as the creation of new products and services in the healthcare industry that were previously not available. As such, HIT is increasingly being viewed as one of the most promising ways in which to improve healthcare operations including patient safety, records management, the efficiency of delivery systems and the overall quality of treatment. Industry practitioners believe that consistent use of technology in the healthcare sector leads to increased healthcare efficiency, a reduction in costs, a decrease in the paperwork involved, the extension of real-time communication, and improvement of healthcare quality (Chaudhry et al., 2006; Esposito, De Santis, Tortora, Chang, & Choo, 2018; Ribitzky et al., 2018).

There have been many recent developments within the healthcare industry that have helped pave a way for blockchain technology in said industry. For instance, there has been significant development in the adoption of electronic gathering of health-related data, cloud computing for data storage, enhanced privacy protection regulations for patient data, and the new opportunities that are continuously emerging in the healthcare industry for data management, as well as the convenience that is created from patients being able to access and share their personal health data (Chen, Ding, Xu, Zheng, & Yang, 2019).

Blockchain technology has been successfully adopted and applied in the financial services industry to improve the security of financial transactions, and particularly those involving digital currencies such as Bitcoin. The same concepts can be borrowed and applied in the healthcare industry to help improve security in terms of how health records and patient information are stored, retrieved and shared among different stakeholders. There have been many studies in the health sector that have evaluated the potential of blockchain technology in said sector (Cyran, 2018).

Alzahrani, A., Alenezi, A., Atlam, H. and Wills, G.
A Framework for Data Sharing between Healthcare Providers using Blockchain.
DOI: 10.5220/0009413403490358
In *Proceedings of the 5th International Conference on Internet of Things, Big Data and Security (IoTBDS 2020)*, pages 349-358
ISBN: 978-989-758-426-8

This research proposes a framework based on the blockchain technology to provide a secure environment for data sharing between healthcare providers in the Kingdom of Saudi Arabia (KSA). It starts by providing analysis of the healthcare industry with a particular focus on the context of the healthcare sector in KSA. Consequently, the research review the health systems currently in place and the general culture of KSA as it relates to the use of technology in the industry. The research also investigates the potential of the blockchain technology in the health sector and how to influence Healthcare Providers in KSA to use it.

This paper is structured in six main sections. The first part of the paper reviews the healthcare information systems and blockchain. The second part discusses how blockchain can address healthcare challenges. Afterward, detailed analysis and discussion of the related work are presented in the fourth section. Whilst section five present the proposed framework and its factors definitions. Finally, the conclusion and future work section are presented in section six.

2 BACKGROUND

In this section a review of healthcare information systems, blockchain and the KSA context are discussed.

2.1 Healthcare Information Systems

Healthcare practices generate extensive amounts of data which can be seen as a data domain where it is regularly accessed, created, or stored on a daily basis (Esposito et al., 2018). Technology can play an important role in boosting the quality of patients' treatment and reducing the cost by using resources such as practitioners and equipment (Esposito et al., 2018). There are different kinds of healthcare technology that are used to achieve different objectives, with the ultimate focus on improving patient outcomes and enhancing patient experience in health facilities.

Healthcare data usually comprises information which is very sensitive for its owners. For instance, patients may be hesitant to share their data and have it used for research purposes despite the positive impact that such data can have on other patients in similar conditions. This is because any inappropriate disclosure of patient data or the identities of the patients can have an impact on their health as well as other social or financial implications concerning them and their employers, and insurance companies among other interested parties (Theodouli, Arakliotis, Moschou, Votis, & Tzovaras, 2018).

The use of centralised data storage in health institutions is considered the main limitation standing in the way of interoperability, because it is considered an issue for healthcare provider where they store all the data/records in databank or one central database. The issues that result from using a central storage database are health data fragmentation, lack of quality of data, low speed access to medical data, and unavailability of system interoperability (Azaria, Ekblaw, Vieira, & Lippman, 2016).

The medicinal services industry, specifically, has been a noteworthy target for information theft, as medical records oftentimes contain private data, e.g. the names, social security numbers , and addresses of patients (Dagher, Mohler, Milojkovic, & Marella, 2018).

In the US, no fewer than 112 million security breaches were enumerated in the medical databases in 2016, with these breaches involving approximately 33% of the medical databases. In the last two decades, an almost $30 billion loss has resulted from these attacks on medical databases. Beside the financial losses, said attacks are clearly a violation of the patients' privacy and their data (Zhang, Schmidt, White, & Lenz, 2018). Thus, there is a need to confront any future incidents, and healthcare data decentralisation using blockchain is a possible way to do so (Mwashuma, 2018).

2.1.1 Privacy in Healthcare

The concerns regarding protection of patients' confidentiality and identity still exist despite the need for data sharing (Terry, 2009). For example, the interaction between medical systems might raise the risk of health information and leakage due to the electronic transmission of data without very secure infrastructure, which may result in serious legal and financial consequences (Downey & Olson, 2013).

Centralised institutions, as shown in Figure 1, both private and public, gather enormous quantities of sensitive and personal information. In terms of the data on individuals which has been stored, these individuals usually have little or no control over said data and how it is used. (Zyskind & Nathan, 2015). In general, both special category data and personal data are vulnerable to attack and misuse, thus meaning they should not be trusted in the hands of intermediaries (Zyskind & Nathan, 2015).

With regard to recent attacks on clinical information in cloud systems, different countries, such as the US (Glaser, 2017) and UK (O'Dowd, 2017) have experienced significant data loss. Keeping patients' personal data in the cloud without encryption will allow the attackers to breach and steal private sensitive data (Al Omar, Bhuiyan, Basu, Kiyomoto, & Rahman, 2019). Sensitive information should be protected and kept safe from trespassers and eavesdroppers (Al Omar, Rahman, Basu, & Kiyomoto, 2017). There have been negative impacts, resulting from breaches, on the overall perception of the healthcare sector, and these impacts threaten to prevent future research which could lead to more rigorous regulatory constraints (Patil & Seshadri, 2014).

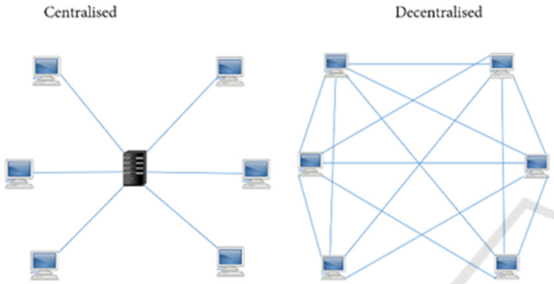

Figure 1: Centralisation vs Decentralisation.

2.1.2 Data Sharing

Currently, centralised data sharing is struggling to fulfil the accessibility, scalability and security requirements of the healthcare sector (Cyran, 2018). In order to offer efficient collaborative treatment and care decisions to the patients, it is essential to provide scalable and secure data exchange. Patients visit multiple and different clinical institutions during their lifetime. The health providers need to keep their patients' conditions and data updated by being able to exchange these patients' information in a timely and private manner (Zhang, White, Schmidt, Lenz, & Rosenbloom, 2018).

Nowadays, almost all heath data is stored in Electronic Medical Records (EMR) systems, although the data mostly remains non-portable (Ivan, 2016). The difficulty in moving and sharing health information in a secure way and in a timely manner has a harmful impact on the care of the patient (Ivan, 2016). Some health entities take the advantage of perceiving data management and use as a competition like it appears in Figure 2. And to the mentioned kind of entities sharing health records will allow the patients to seek care services from different institutions but owning health record by providers mostly will make the patient keep come and stick to same clinic. In addition, health providers consider patients' medical data to be their own property. This is true with regard to the legal aspects, yet it sometimes creates costly or unnecessary barriers for patients who need or want to give their own medical records to another institution (Ivan, 2016).

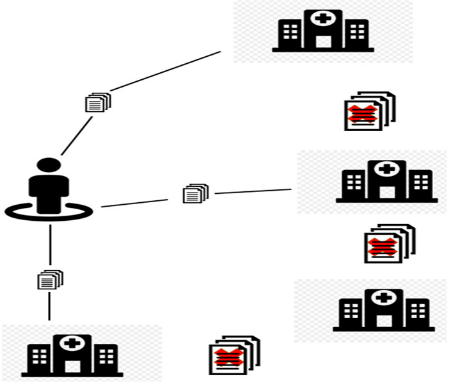

Figure 2: Lack of sharing data between hospitals.

Health providers sharing medical records between one another reduces the waste and cost which may, for instance, occur when there is duplicate testing because the patients visit different clinics (Engelhardt, 2017). However, entities are often unwilling to share medical data either because of certain privacy concerns, or just simply because they are afraid this will give other institutions a competitive advantage (Vest & Gamm, 2010).

2.1.3 Healthcare Systems in KSA

The level of adoption of Electronic Health Records (EHR) systems in hospitals in the KSA is currently poorly known. Furthermore, the determinants of the adoption of HIT have not yet been quantified. In addition, unlike most countries in the West, KSA does not have any data protection laws (Aldosari, 2014). The existing Anti-Cyber Crime Law that was issued and approved in 2007 is considered very general and unclear (Commission, 2017).

The culture of KSA is another important factor for consideration when evaluating the healthcare systems in the country. This is because several studies have indicated that local culture is one of the most important barriers facing the adoption of new technology and the use of online services in the country (Hwang, Li, Shen, & Chu, 2004; Schneider, 2010). This can be attributed to the lack of awareness and knowledge of existing technologies and how they work. As a result, government organisations and agencies in KSA encounter several problems related to acceptance of new technologies (Khater & Rashed, 2017).

2.1.4 Challenges of Healthcare Systems in KSA

In the context of KSA, medical information is one of the most targeted assets even more than personal data in the healthcare domain. A recent survey conducted by (Accenture, 2017) showed that a significant majority of consumers have personally encountered a breach of their medical data. The health data of 75% of those surveyed was breached, while only 32% claimed that it happened to their personal information. This showed that the number of breaches in KSA was nearly three times higher (35%) compared to other surveyed countries. The most common places for this to happen, as the above study showed, were hospitals (43%), the office of the physician (25%) and the pharmacy (24%).

Europe and Northern America have a set of laws in place to ensure that personal data is secured and protected, while KSA does not have any laws regarding data protection, nor any information for data security violations. Despite this, there is an Anti-Cyber Crime law that was issued and approved in 2007, although it is considered a quite general and unclear law (Commission, 2017).

Data Sharing is one of the most significant challenges in KSA. Most hospitals and health facilities in the country find it difficult to regularly update patient records. Recent studies indicated that only 16% of the hospitals in the country have implemented EHR (Bah et al., 2011). Most public hospitals still rely on paper-based systems for managing patient records, with evidence suggesting that the adoption of technology in these hospitals is quite rare (Aljarullah, Crowder, & Wills, 2017).

2.2 Blockchain

Blockchain can be outlined as a distributed ledger that is immutable and shared by peers in the network, where records of transactions or events are appended in a chronological order (Agbo, Mahmoud, & Eklund, 2019).

The blockchain technology is considered an efficient enhancement tool for identity verification and integrity of data, and thus it provides users with consistent and trustworthy data in the cloud environment (Liu, Yu, Chen, Xu, & Zhu, 2017). In addition, blockchain is a robust instrument that boosts governments' information resource information performance. The peer-to-peer (P2P) decentralised data sharing system advances the efficiency of sharing and decreases possible costs related to data (Wang, Liu, & Han, 2017).

It facilitates engagement, smart contracts and agreements, while also making the cyber security feature more robust (Ahram, Sargolzaei, Sargolzaei, Daniels, & Amaba, 2017). In addition, blockchain can be defined as blocks that are timestamped and chained together using hashing cryptography. These blocks are sealed in immutable and secure manner (Aste, Tasca, & Di Matteo, 2017; Roehrs, da Costa, & da Rosa Righi, 2017).

2.2.1 Security in Blockchain

The technology environment continues to develop and change, with the threats posed by hackers, viruses, criminals and terrorists against information security (IS) consistently increasing (ITGI, 2006). Blockchain technology is showing some potential in healthcare in terms of helping to overcome challenges regarding data security, sharing, privacy and storage (Engelhardt, 2017). One of the most important requirements in the healthcare industry is interoperability, which is the ability of multiple parties, whether machine or human, to exchange information or data consistently and in an efficient way (Al Ridhawi, Aloqaily, Kantarci, Jararweh, & Mouftah, 2018; Al Ridhawi, Aloqaily, Kotb, Al Ridhawi, & Jararweh, 2018; Iroju, Soriyan, Gambo, & Olaleke, 2013; Mead, 2006).

The blockchain infrastructure ensures that the data stored on the network is immutable and has an auditable history. This concept is vital in healthcare because it would help preserve the integrity of patient data by ensuring that no other person can access and alter said data. All transactions involving the specific set of data are traceable, which facilitates auditing of the transition processes on the network (Mikula & Jacobsen, 2018).

2.2.2 Blockchain in KSA

Blockchain is considered an emerging technology and has not yet been adopted nor applied in the KSA as far as we know. Based on the search result regarding blockchain in KSA, there was only one result that discussed VAT in the financial system. In the mentioned study the author proposed a system containing a transparent database for VAT transactions to deduct the tax and store it on a peer-to-peer network (Alkhodre et al., 2019). However, the proposed solution has not been implemented in the real world yet.

3 HOW BLOCKCHAIN CAN ADDRESS THE HEALTHCARE SYSTEMS CHALLENGES

The existing systems that depend on a single authority to store encrypted data will be vulnerable to attack, and attackers can concentrate their effort on a single target to perpetrate DoS attacks, inject malicious data, and extort data through theft or blackmailing. The management of medical data in a safe and accurate way will lead to the development of digital health (Ichikawa, Kashiyama, & Ueno, 2017).

Government entities can provide better services in healthcare by keeping the medical records of patients, which can then be shared with other service providers (Alketbi, Nasir, & Talib, 2018).

In addition, there are some advantages when it comes to the implementation of blockchain technology in healthcare institutions. One of these is the management of electronic medical records for patients. Nowadays, patient data is stored in a secure way in many places, yet scattered between many organisations, clinics and insurance providers, without full access to a shared database of patients (Skiba, 2017).

The other benefits of applying blockchain in healthcare institutions are: immutability and verifiability for transactions, transparency, tamper resistance, and integrity of distributed sensitive health information. Basically this can be achieved by using a consensus protocol and cryptographic mechanisms such as digital signatures and hashing (Dubovitskaya, Xu, Ryu, Schumacher, & Wang, 2017).

Blockchains are decentralised, meaning that they do not need the authority or trust of individuals of the network or the group. The reason that the system does not require trust is because each node has a complete copy of all the historic information available and just by achieving the majority consensus more data will be added to the chain of prior information. Therefore, blockchain has the upper hand over the current security measures (Taylor, Dargahi, Dehghantanha, Parizi, & Choo, 2019).

The blockchain addresses many issues with current health IT models, which include security, and especially data integrity and privacy, and immutability, which assures identities, thus creating a very strong audit trail and subsequently improving healthcare-related security either for patients or providers (Brodersen et al., 2016).

It is foreseeable that blockchain technology will benefit patients who interact with systems of healthcare by avoiding routine registration processes and decreasing their waiting time. Moreover, by providing immutable and transparent personalised medical records that can be accessed from anywhere (universal EMR) it will decrease paperwork, cost and overheads (Rabah, 2017).

4 RELATED WORK

In this section reviews of the related works on healthcare systems that based on blockchain are critically reviewed.

Gem Health Network (GHN) allows health providers to share health information and data based on blockchain technology. GHN was developed based on Ethereum blockchain technology to create a secure infrastructure in which there is a shared ledger system where new transactions and records are maintained, thus removing the challenges resulting from centralised storage. This system gives patients significant control of their data while also allowing health providers access to all relevant information in real time (Mettler, 2016).

In 2011, there was a collaboration between the country of Estonia and Guardtime, the latter of which uses blockchain technology to operate a healthcare platform that now secures millions of records (Vazirani, O'Donoghue, Brindley, & Meinert, 2019). Thus, Estonia has shown that operating a complete public health infrastructure using blockchain technology is achievable (Mettler, 2016). Moreover, in this system the patients own and control the access to their healthcare data (Kim, Kuo, & Ohno-Machado, 2017).

MedRec is a blockchain-based decentralized record management system to handle EHR was designed to manage issues such as authentication, confidentiality, accountability and data sharing in managing healthcare records and patient data. The technology also provides an immutable log of all transactions involving a patient's information is created and provided to the patient (Ekblaw, Azaria, Halamka, & Lippman, 2016). However, the MedRec system does not store patients' health records. The system uses blockchain technology to store the record's signature. The signature provides an assurance that the record’s unaltered copy is obtained (Azaria et al., 2016; Ekblaw et al., 2016).

Medshare was introduced by Xia et al. (2017) to address the issues of sharing medical data. This system is built using blockchain technologywhich is secured and safe for health data exchange between untrusted entities. The aforementioned design uses smart contracts and control mechanism to track the data behaviour in an effective manner and repeal the access to the entities on detection of violation the permissions on data. Healthbank offers users a platform where they can store and manage their medical information in a secure environment and also make it available for medical research in exchange for financial compensation. This company is working on empowering patients to have full control of their data by using blockchain technology for transaction validation and verification.

Ancile is a framework built on Etherum blockchain and uses smart contracts for EHR management that gives the ownership and the control of EMRs to the patients. It securely controls the access to the documents and keeps tracking of how records are used, transfer records in a secure way, and reduce unauthorized parties' ability to obtain PHI. Another permissioned blockchain framework proposed by Dubovitskaya et al. (2017) for sharing and managing cancer patients' medical records. In the design to authenticate registered users a membership service employed using a username/password scheme. The patient identity was created by using a combination of personally identifying information encrypted for security including names, date of birth, social security number and zip code. And for the medical data, a secure cloud server used to upload them with access managed by the logic of blockchain.

5 PROPOSED FRAMEWORK

This section investigate different framework factors that influence the use of technology in healthcare. While there have been many revolutionary technologies in the past, not all of them have been adopted with ease. New technologies, such as blockchain, are continuously being studied in terms of how they can help improve the health sector. The targeted users, such as healthcare professionals and administrators, must be convinced that the technology will be useful in their line of work and that it will enhance their operations in the health sector.

5.1 Framework Development

The research framework was constructed in three stages, as shown in Figure 3. The first stage involved a literature review, which was conducted in order to collect the influences that affect people's use of technology and sharing data between healthcare providers. This can be beneficial in pointing out the affecting factors that contribute to the use of technology with respect to healthcare systems. The second stage is to collect the relevant factors that are related to data sharing from the previous stage. The final stage is grouping the factors that affect the using blockchain in healthcare systems according to the practitioners in Saudi hospitals, into categories and components.

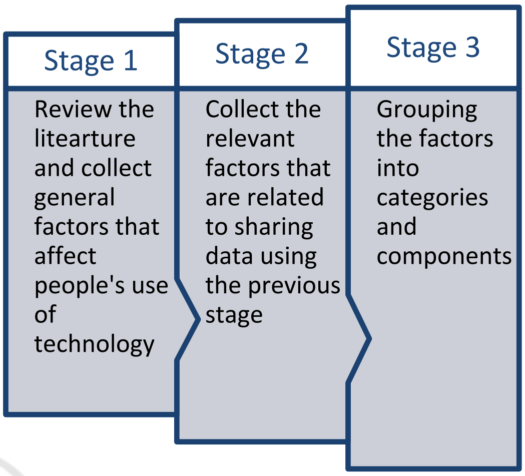
Stage 1
Review the litearture and collect general factors that affect people's use of technology
Stage 2
Collect the relevant factors that are related to sharing data using the previous stage
Stage 3
Grouping the factors into categories and components

Figure 3: The framework development stages.

5.2 Sharing Data between Healthcare Providers Framework (SDHPF)

This framework is divided and organised into three main categories, as illustrated in Figure 4, namely healthcare systems, security, and blockchain.

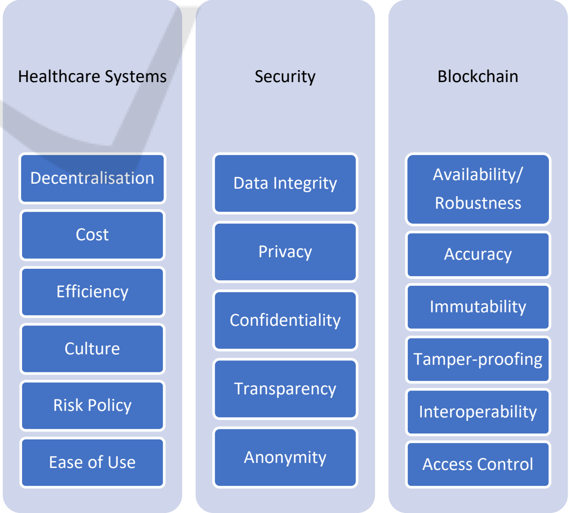

Figure 4: The proposed SDHPF.

5.2.1 Factors Related to Healthcare Systems

In this section the factors that are related to healthcare systems are defined.

Decentralisation: enables distributed environment between the nodes, and the data can be recorded stored and updated without relying on a central authority anymore (Agbo et al., 2019; Alhadhrami, Alghfeli, Alghfeli, Abedlla, & Shuaib, 2017; Hölbl, Kompara, Kamišalić, & Nemec Zlatolas, 2018; Khezr, Moniruzzaman, Yassine, & Benlamri, 2019; Macrinici, Cartofeanu, & Gao, 2018; Mwashuma, 2018; Vazirani et al., 2019).

Cost: blockchain will help to reduce cost that could result in the current systems by moving the records between entities and reducing the administrative cost by eliminating the third party (Engelhardt, 2017; Khezr et al., 2019; Mwashuma, 2018; Rabah, 2017; Vazirani et al., 2019).

Efficiency: repeating tests and unavailability of data could be dangerous because these factors might delay the treatment for the patient as well as increasing the cost. Moreover, sending data in traditional ways, e.g. email, can cause security risks, unlike blockchain, the latter of which has great potential for reducing cost and the production of repetitive registrations while also improving the treatment outcomes (Engelhardt, 2017; Rabah, 2017; Vazirani et al., 2019).

Culture: culture can be considered a huge difficulty that might face the adoption and acceptance of blockchain, and therefore explaining the benefits of blockchain is necessary considering that most people in KSA prefer to contact the government through traditional methods (Abdullah, Rogerson, Fairweather, & Prior, 2006; Hwang et al., 2004; Khater & Rashed, 2017; Schneider, 2010).

Risk Policy: making the policy clear enough to the patients and using smart contracts will help to make the policy suitable for the patients, thus motivating them to be more involved in blockchain technology (Commission, 2017; Khezr et al., 2019).

Ease of Use: this involves showing the system in a way that motivates practitioners such as doctors to use to the technology instead of the basic method (papers), so as to reduce the cost, waiting time, and improve the treatment outcomes (Davis, Bagozzi, & Warshaw, 1989; Venkatesh & Davis, 2000).

5.2.2 Factors Related to Security

The following introduce the factors that are related to the security category in the framework.

Data Integrity: the immutable property of blockchain will guarantee the integrity of the data because, once the data is saved on blockchain, it cannot be altered, corrupted, or even deleted (Alhadhrami et al., 2017; Alketbi et al., 2018; Engelhardt, 2017; Rabah, 2017; Vazirani et al., 2019).

Privacy: blockchain will be more secured, since all data on blockchain is encrypted, and using the symmetric encryption will help to keep the identity of the patient anonymous, thus protecting his/her privacy (Agbo et al., 2019; Engelhardt, 2017; Vazirani et al., 2019).

Confidentiality: confidentiality of the patient is assured because the data is encrypted using the symmetric technique by default, and this will maintain the anonymity of patients and protect the information from hacking. Using blockchain will make data/records available, and this will decrease the issues that result from storing the data of patients locally in each hospital, such as repeating the tests and basic paperwork (Alhadhrami et al., 2017; Rabah, 2017; Sankar, Sindhu, & Sethumadhavan, 2017).

Transparency: blockchain can improve communication and data transparency between clinics and the data will be updated and therefore trusted and accessed from anywhere (Azaria et al., 2016; Khezr et al., 2019; Linn & Koo, 2016; Mwashuma, 2018).

Anonymity: eliminating the third party will smooth communication and data transference between nodes, while the identities of individuals remain anonymous because of data encryption, which makes the system secure and more reliable. In addition, access is limited to only fully trusted nodes when it comes to sensitive information about the patient (Engelhardt, 2017; Hölbl et al., 2018; Mwashuma, 2018).

5.2.3 Factors Related to Blockchain

The following define the factors that are related to the blockchain category in the framework.

Availability/ Robustness: blockchain enables the replication of data or records in multiple nodes, which ensure that the records that have been stored on blockchain are available; indeed, this makes the system flexible against data hacking, data loss or data corruption (Chowdhury, Colman, Kabir, Han, & Sarda, 2018; Hölbl et al., 2018; Taylor et al., 2019).

Accuracy: the records will be accurate regarding the consensus of nodes in blockchain, because it is almost impossible for the data in the records added on blockchain to be changed, tamper with or deleted (Engelhardt, 2017; Vazirani et al., 2019).

Immutability: one of the most important properties of blockchain is that the records will be reserved forever after nodes majority consensus, and it will become very difficult for anyone to tamper with or modify said records (Agbo et al., 2019; Engelhardt, 2017; Mwashuma, 2018; Rabah, 2017; Taylor et al., 2019; Vazirani et al., 2019).

Tamper-proofing: after data is added to the blockchain, due to the encryption and digital signature it cannot be changed, and if anything has been modified or removed it will be easy to detect (Dai, Shi, Meng, Wei, & Ye, 2017).

Interoperability: one of the potentials provided by blockchain and needed most by healthcare systems is to exchange patients' data freely in a secure way and thus ensure the decreasing cost, efficiency, and privacy (Khezr et al., 2019; Mwashuma, 2018; Vazirani et al., 2019).

Access Control: this will provide the ability to track any action that has been carried out in the system and identify which user carried it out, thus limiting the access to completely trusted nodes to handle critical (Abouelmehdi, Beni-Hssane, Khaloufi, & Saadi, 2017; Vazirani et al., 2019).

6 CONCLUSIONS

In summary, the primary objective of this research was to provide an overview of the potential of blockchain technology in the healthcare industry. The use of technology in providing healthcare services comes with a lot of considerations that must be analysed comprehensively to make the technologies effective. New healthcare information technologies focus on providing an avenue through which the health sector can keep growing and improving while at the same time maintaining the quality levels through minimising the costs of accessing healthcare and simultaneously improving patient experience in healthcare facilities. The healthcare industry has been suffering from inefficiencies in the handling of data. Many patients and healthcare providers are frustrated with the numerous hurdles when it comes to obtaining current real-time patient information.

In conclusion, blockchain is a possible solution through which to secure the health data of patients. The question will be whether the technology is too early in its infancy or if the cost to set up the infrastructure is too high at this moment. The most important hurdle of all is to implement this technology within the parameters set forth by regulators in the healthcare space. Therefore, the primary target of this research is to investigate the factors that influence healthcare providers to share data using blockchain which has led to proposeing the SDHPF. In terms of future work the next step is to have the proposed framework reviewed by a number of experts. Once the framework is reviewed by a number of relevant experts, a survey will be distributed to a number of practitioners in the field of blockchain and healthcare systems to confirm the framework which will be then used as a case study in the real world.

REFERENCES

Abdullah, A., Rogerson, S., Fairweather, N. B., & Prior, M. (2006). The motivations for change towards e-government adoption: Case studies from Saudi Arabia. Paper presented at the E-government Workshop.

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. *Procedia Computer Science, 113*, 73-80.

Accenture. (2017). The impact of healthcare cybersecurity on SAUDI ARABIAN consumers.

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). *Blockchain* Technology *in Healthcare: A Systematic Review.* Paper presented at the Healthcare.

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). *Blockchain technology innovations.* Paper presented at the 2017 IEEE Technology & Engineering Management Conference (TEMSCON).

Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future generation computer systems, 95*, 511-521.

Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017). *Medibchain: A blockchain based privacy preserving platform for healthcare data.* Paper presented at the International conference on security, privacy and anonymity in computation, communication and storage.

Al Ridhawi, I., Aloqaily, M., Kantarci, B., Jararweh, Y., & Mouftah, H. T. (2018). A continuous diversified vehicular cloud service availability framework for smart cities. *Computer Networks, 145*, 207-218.

Al Ridhawi, I., Aloqaily, M., Kotb, Y., Al Ridhawi, Y., & Jararweh, Y. (2018). A collaborative mobile edge computing and user solution for service composition in 5G systems. *Transactions on Emerging Telecommunications Technologies, 29*(11), e3446.

Aldosari, B. (2014). Rates, levels, and determinants of electronic health record system adoption: A study of hospitals in Riyadh, Saudi Arabia. *International journal of medical informatics, 83*(5), 330-342.

Alhadhrami, Z., Alghfeli, S., Alghfeli, M., Abedlla, J. A., & Shuaib, K. (2017, 21-23 Nov. 2017). *Introducing blockchains for healthcare.* Paper presented at the 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA).

Aljarullah, A., Crowder, R., & Wills, G. (2017). *A framework for the adoption of EHRs by primary healthcare physicians in the kingdom of Saudi Arabia.*

Paper presented at the 2017 International Conference on Information Society (i-Society).

Alketbi, A., Nasir, Q., & Talib, M. A. (2018). *Blockchain for government services—Use cases, security benefits and challenges.* Paper presented at the 2018 15th Learning and Technology Conference (L&T).

Alkhodre, A., Jan, S., Khusro, S., Ali, T., Alsaawy, Y., & Yasar, M. (2019). A Blockchain-based Value Added Tax (VAT) System: Saudi Arabia as a Use-Case.

Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry. *Computer, 50*(9), 18-28.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). *Medrec: Using blockchain for medical data access and permission management.* Paper presented at the 2016 2nd International Conference on Open and Big Data (OBD).

Bah, S., Alharthi, H., El Mahalli, A. A., Jabali, A., Al-Qahtani, M., & Al-kahtani, N. (2011). Annual survey on the level and extent of usage of electronic health records in government-related hospitals in Eastern Province, Saudi Arabia. *Perspectives in health information management/AHIMA, American Health Information Management Association, 8*(Fall).

Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., Truscott, A., & Accenture, L. (2016). Blockchain: Securing a new health interoperability experience. *ed: Accenture LLP*, 1-10.

Chaudhry, B., Wang, J., Wu, S., Maglione, M., Mojica, W., Roth, E., . . . Shekelle, P. G. (2006). Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. *Annals of internal medicine, 144*(10), 742-752.

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. *Journal of medical systems, 43*(1), 5.

Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarda, P. (2018, 1-3 Aug. 2018). *Blockchain Versus Database: A Critical Analysis.* Paper presented at the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).

Commission, C. a. I. T. (2017). Anti-Cyber Crime Law.

Cyran, M. A. (2018). Blockchain as a foundation for sharing healthcare data. *Blockchain in Healthcare* Today.

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society, 39*, 283-297.

Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017, 11-13 Nov. 2017). *From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues.* Paper presented at the 2017 4th International Conference on Systems and Informatics (ICSAI).

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science, 35*(8), 982-1003.

Downey, A. S., & Olson, S. (2013). *Sharing clinical research data: workshop summary*: National Academies Press.

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). *Secure and trustable electronic medical records sharing using blockchain.* Paper presented at the AMIA Annual Symposium Proceedings.

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). *A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data.* Paper presented at the Proceedings of IEEE open & big data conference.

Engelhardt, M. A. (2017). Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Technology Innovation Management Review, 7*(10).

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.-K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing, 5*(1), 31-37.

Glaser, A. (2017). US hospitals have been hit by the global ransomware attack. *Retrieved, 20*, 2018.

Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. *Symmetry, 10*(10), 470.

Hwang, M.-S., Li, C.-T., Shen, J.-J., & Chu, Y.-P. (2004). Challenges in e-government and security of information. *Information & Security, 15*(1), 9-20.

Ichikawa, D., Kashiyama, M., & Ueno, T. (2017). Tamper-resistant mobile health using blockchain technology. *JMIR mHealth and uHealth, 5*(7), e111.

Iroju, O., Soriyan, A., Gambo, I., & Olaleke, J. (2013). Interoperability in healthcare: benefits, challenges and resolutions. *International Journal of Innovation and Applied Studies, 3*(1), 262-270.

ITGI. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management*: ISACA.

Ivan, D. (2016). *Moving toward a blockchain-based method for the secure storage of patient records.* Paper presented at the ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST.

Khater, A., & Rashed, N. (2017). *A model of a private sector organisation's intention to adopt cloud computing in the Kingdom of Saudi Arabia.* University of Southampton,

Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Applied Sciences, 9*(9), 1736.

Kim, H.-E., Kuo, T.-T., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the*

American Medical Informatics Association, 24(6), 1211-1220. doi:10.1093/jamia/ocx068

Linn, L. A., & Koo, M. B. (2016). *Blockchain for health data and its potential use in health it and health care related research.* Paper presented at the ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST.

Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). *Blockchain based data integrity service framework for IoT data.* Paper presented at the 2017 IEEE International Conference on Web Services (ICWS).

Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*.

Mead, C. N. (2006). Data interchange standards in healthcare it-computable semantic interoperability: Now possible but still difficult. do we really need a better mousetrap? *Journal of Healthcare Information Management, 20*(1), 71.

Mettler, M. (2016). *Blockchain technology in healthcare: The revolution starts here.* Paper presented at the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom).

Mikula, T., & Jacobsen, R. H. (2018). *Identity and access management with blockchain in electronic healthcare records.* Paper presented at the 2018 21st Euromicro Conference on Digital System Design (DSD).

Mwashuma, E. W. (2018). Towards universal healthcare coverage through adoption of blockchain technology: a literature review. *Journal of Health Informatics in Africa, 5*(2).

O'Dowd, A. (2017). Major global cyber-attack hits NHS and delays treatment. *BMJ: British Medical Journal (Online), 357*.

Patil, H. K., & Seshadri, R. (2014). *Big data security and privacy issues in healthcare.* Paper presented at the 2014 IEEE international congress on big data.

Rabah, K. (2017). Challenges & opportunities for blockchain powered healthcare systems: A review. *Mara Research Journal of Medicine & Health Sciences-ISSN 2523-5680, 1*(1), 45-52.

Ribitzky, R., Clair, J. S., Houlding, D. I., McFarlane, C. T., Ahier, B., Gould, M., . . . Clauson, K. A. (2018). Pragmatic, interdisciplinary perspectives on blockchain and distributed ledger technology: paving the future for healthcare. *Blockchain in Healthcare Today*.

Roehrs, A., da Costa, C. A., & da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of biomedical informatics, 71*, 70-81.

Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017). *Survey of consensus protocols on blockchain applications.* Paper presented at the 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS).

Schneider, R. M. (2010). *A comparison of information security risk analysis in the context of e-government to criminological threat assessment techniques.* Paper presented at the 2010 Information Security Curriculum Development Conference.

Skiba, D. J. (2017). The potential of Blockchain in education and health care. *Nursing education perspectives, 38*(4), 220-221.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2019). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*.

Terry, M. (2009). Medical identity theft and telemedicine security. *Telemedicine and e-Health, 15*(10), 928-933.

Theodouli, A., Arakliotis, S., Moschou, K., Votis, K., & Tzovaras, D. (2018). *On the design of a Blockchain-based system to facilitate Healthcare Data Sharing.* Paper presented at the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).

Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019). Implementing Blockchains for Efficient Health Care: Systematic Review. *J Med Internet Res, 21*(2), e12439. doi:10.2196/12439

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science, 46*(2), 186-204.

Vest, J. R., & Gamm, L. D. (2010). Health information exchange: persistent challenges and new strategies. *Journal of the American Medical Informatics Association, 17*(3), 288-294.

Wang, L., Liu, W., & Han, X. (2017). *Blockchain-based government information resource sharing.* Paper presented at the 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS).

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757-14767.

Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. In *Advances in Computers* (Vol. 111, pp. 1-41): Elsevier.

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. *Computational and structural biotechnology journal, 16*, 267-278.

Zyskind, G., & Nathan, O. (2015). *Decentralizing privacy: Using blockchain to protect personal data.* Paper presented at the 2015 IEEE Security and Privacy Workshops.